ÁLGEBRA LINEAL Y ESTRUCTURAS MATEMÁTICAS

22 de Noviembre de 2018

Alumno:____________________________________ **D.N.I.:**_______________ **Grupo F**

Ejercicio 1. *Responde a las siguientes cuestiones:*

1. *¿Qué números hay con dos cifras que al pasarlos a base 7 se escriben con las mismas cifras, pero en orden iverso? (no se admite una búsqueda por fuerza bruta).*
2. *¿Existe el inverso de* 901 *en* $\mathbb{Z}_{1649}$*? ¿Y el de* 127 *en* $\mathbb{Z}_{1127}$*? En los casos en que exista, calcúlalo.*
3. *Realiza en* $\mathbb{Z}_{77}$ *los siguientes cálculos:* $37 \cdot 21$, 54^{362}, $15 \cdot 32 - 22^4 \cdot 11$, $21 \cdot 22$.
4. *Calcula, en cada caso, todas las soluciones de las siguientes ecuaciones en* $\mathbb{Z}_{35}$.
   - $23(x+4) + 3^{-1} = 4x + 5$.
   - $8(x+5) + 3x = 4(8x-3) + 1$.
   - $4(5x+2) + 5x - 3 = 4x - 2$.

Solución:

1. Sea x un tal número. Supongamos que sus cifras (en decimal) son a, b. El número es entonces $x = 10 \cdot a + b$. Sabemos que si lo expresamoe en base 7, sus cifras son b, a, por tanto, $x = 7 \cdot b + a$. Entonces:

$$10 \cdot a + b = 7 \cdot b + a; \quad 10 \cdot a - a = 7 \cdot b - b; \quad 9 \cdot a = 6 \cdot b; \quad 3 \cdot a = 2 \cdot b.$$

   Por tanto, $2b$ tiene que ser múltiplo de 3, luego b también es múltiplo de 3. En tal caso, b puede valer 3 ó 6. Mayor que 6 no puede ser, pues b es la cifra de un número en base 7. Y 0 tampoco puede ser, pues en tal caso estaríamos hablando del número $x = 0$, que no tiene dos cifras.

   Si $b = 3$ entonces $a = 2$, mientras que si $b = 6$, a vale 4.

   Los números son entonces 23 y 46. Podemos comprobar fácilmente que $23 = 32)_7$ y $46 = 64)_7$.

2. Para ver si 901 tiene inverso en $\mathbb{Z}_{1649}$ calculamos el máximo común divisor de 1649 y 901. Nos valemos del algoritmo de Euclides.

   $1649 = 901 \cdot 1 + 748$. Luego $\text{mcd}(1649, 901) = \text{mcd}(901, 748)$.
   $901 = 748 \cdot 1 + 153$. Luego $\text{mcd}(1649, 901) = \text{mcd}(748, 153)$.
   $748 = 153 \cdot 4 + 136$. Por tanto, $\text{mcd}(1649, 901) = \text{mcd}(153, 136)$.
   $153 = 136 \cdot 1 + 17$. Tenemos entonces que $\text{mcd}(1649, 901) = \text{mcd}(136, 17)$.
   $136 = 17 \cdot 8 + 0$. Y entonces $\text{mcd}(1649, 901) = \text{mcd}(17, 0) = 17$.

   Como $\text{mcd}(1649, 901) \neq 1$ no existe el inverso que nos piden.

   Para el inverso de 127 en $\mathbb{Z}_{1127}$ procedemos de igual forma:

$$\begin{array}{ll} 1127 = 127 \cdot 8 + 111 & \text{mcd}(1127, 127) = \text{mcd}(127, 111). \\ 127 = 111 \cdot 1 + 16 & \text{mcd}(1127, 127) = \text{mcd}(111, 16). \\ 111 = 16 \cdot 6 + 15 & \text{mcd}(1127, 127) = \text{mcd}(16, 15). \\ 16 = 15 \cdot 1 + 1 & \text{mcd}(1127, 127) = \text{mcd}(15, 1) = 1. \end{array}$$

   Puesto que en esta ocasión el máximo común divisor vale 1, sí existe el inverso. Lo calculamos con el algoritmo extendido de Euclides, para lo cual aprovechamos las divisiones que ya hemos realizado.

1127		0
127		1
111	8	v_1
16	1	v_2
15	6	v_3
1	1	v_4

$v_1 = 0 - 8 \cdot 1 = -8$
$v_2 = 1 - 1 \cdot (-8) = 9$
$v_3 = -8 - 6 \cdot 9 = -62$
$v_4 = 9 - 1 \cdot (-62) = 71$

1127		0
127		1
111	8	-8
16	1	9
15	6	-62
1	1	71

Tenemos que $127^{-1} = 71$.

3. Calculamos:

   - $37 \cdot 21 = 777 = 7$ (ya que $777 = 77 \cdot 10 + 7$).
   - Para calcular 54^{362} comprobamos primero que $\mathrm{mcd}(77, 54) = 1$. Esto es cierto, pues $77 = 7 \cdot 11$ mientras que $54 = 2 \cdot 3^3$, y vemos que no tienen divisores comunes. En tal caso, tenemos que $54^{\varphi(77)} = 1$, y $\varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$.

     Por tanto, $54^{60} = 1$, y puesto que $362 = 60 \cdot 6 + 2$ tenemos que $54^{362} = 54^2 = 2916 = 67$.
   - $15 \cdot 32 - 22^4 \cdot 11 = 480 - 234256 \cdot 11 = 18 - 2576816 = 18 - 11 = 7$.
   - $22 \cdot 21 = 462 = 0$.

4. Resolvemos las tres ecuaciones:

   - Comenzamos por $23(x + 4) + 3^{-1} = 4x + 5$.

     $23(x + 4) + 3^{-1} = 4x + 5$
     $23x + 92 + 12 = 4x + 5$
     $23x - 4x = 5 - 12 - 92$
     $19x = -99$
     $19x = 6$
     $x = 6 \cdot 24 = 144$
     $x = 4$

35		0
19		1
16	1	-1
5	1	2
1	5	-11

     19^{-1} mód $35 = -11 = 24$

   - Continuamos por la ecuación $8(x + 5) + 3x = 4(8x - 3) + 1$.

     $8(x + 5) + 3x = 4(8x - 3) + 1.$
     $8x + 40 + 3x = 32x - 12 + 1.$
     $8x + 3x - 32x = -12 + 1 - 40.$
     $-21x = -51.$
     $14x = 19.$

     Esta ecuación es equivalente a $14x \equiv 19$ mód 35. Puesto que $\mathrm{mcd}(35, 14) = 7$ y 19 no es múltiplo de 7, esta congruencia no tiene solución. Luego la ecuación inicial tampoco tiene.

   - Terminamos con la ecuación $4(5x + 2) + 5x - 3 = 4x - 2$.

     $4(5x + 2) + 5x - 3 = 4x - 2.$
     $20x + 8 + 5x - 3 = 4x - 2.$
     $20x + 5x - 4x = -2 + 3 - 8.$
     $21x = -7.$
     $21x = 28.$

     Ahora esta ecuación es equivalente a $21x \equiv 28$ mód 35. Como $\mathrm{mcd}(21, 35) = 7$ y 7 es divisor de 28, la congruencia tiene solución. Dividimos todo por 7 y nos queda $3x \equiv 4$ mód 5, que resolvemos multiplicando por $2 = 3^{-1}$: $x \equiv 3$ mód 5, es decir, $x = 3 + 5k$.

     Como $x \in \mathbb{Z}_{35}$, los posibles valore de x son $x = 3$, $x = 8$, $x = 13$, $x = 18$, $x = 23$, $x = 28$, $x = 33$. La siguiente sería $x = 38 = 3$, que ya la tenemos.

Ejercicio 2. *Elegir una de las dos opciones siguientes:*

1. *En cada uno de los siguientes apartados se pide una solución de la ecuación diofántica* $36x+28y+63z=5$ *que cumpla la condición que se dice. Si no es posible dar esa solución, hay que justificarlo:*
   - x *debe ser mayor que* 20.
   - z *debe ser menor que* -10.
   - *Tanto* x *como* y *deben ser mayores que* 3.
   - z *debe ser múltiplo de* 4.
2. *Tenemos que ir a una oficina de correos a enviar un total de* 17 *paquetes. Estos paquetes están divididos en dos tipos, que denominaremos* `Tipo A` *y* `Tipo B`*. Mandar un paquete* `Tipo B` *nos cuesta* 35 *céntimos más que enviar un paquete tipo A.*

   El envío total nos cuesta $54'5$ *euros. ¿Cuántos paquetes enviamos de cada tipo, y cuál es el precio de cada uno de ellos?*

Solución:
Resolvemos cada una de las dos opciones:

1. Tenemos que buscar varias soluciones de la ecuación diofántica $36x+28y+63z=5$. Puesto que $\mathrm{mcd}(36,28,63)=1$ (compruébese), la ecuación tiene solución.

   Calculamos la solución general y luego particularizamos a cada uno de los casos:

   Consideramos para cada z la ecuación (en las variables x e y) $36x+28y=5-63z$. Para que esta ecuación tenga solución, es necesario que $5-63z$ sea múltiplo del máximo común divisor de 36 y 28. Puesto que $\mathrm{mcd}(36,28)=4$, los valores de z para los que tiene solución son aquellos que verifican que $5-63z\equiv 0 \text{mód } 4$.

   Resolvemos esta congruencia:

   $5-63z\equiv 0 \text{ mód } 4.$
   $-63z\equiv -5 \text{ mód } 4.$
   $z\equiv 3 \text{ mód } 4.$
   $z=3+4k : k\in\mathbb{Z}.$

   Para estos valores de z ($z=\cdots-5,-1,3,7,11\cdots$) la ecuación tiene solución. Sustituimos z y tenemos:

   $$36x+28y=5-63(3+4k);\quad 36x+28y=5-189-252k;\quad 36x+28y=-184-252k;\quad 9x+7y=-46-63k.$$

   Y esto lo escribimos como $9x\equiv -46-63k$ mód 7. Ahora resolvemos esta congruencia.

   $9x\equiv -46-63k \text{ mód } 7.$
   $2x\equiv 3+0k \text{ mód } 7.$
   $4\cdot 2x\equiv 4\cdot 3 \text{ mód } 7.$
   $x\equiv 5 \text{ mód } 7.$
   $x=5+7k' : k'\in\mathbb{Z}.$

   Una vez que hemos calculado x y z, sustituimos en la ecuación inicial y despejamos y.

   $36x+28y+63z=5.$
   $28y=5-36x-63z.$
   $28y=5-36(5+7k')-63(3+4k).$
   $28y=5-36\cdot 5-36\cdot 7k'-63\cdot 3-63\cdot 4k.$
   $28y=5-180-189-252k-252k'.$
   $28y=-364-252k-252k'.$
   $y=\frac{-364-252k-252k'}{28}.$
   $y=-13-9k-9k'.$

Y con esto ya tenemos la solución general:

$$\begin{array}{rcrcrcr} x & = & 5 & & & + & 7k' \\ y & = & -13 & - & 9k & - & 9k' \\ z & = & 3 & + & 4k & & \end{array}$$

Y ahora elegimos las soluciones que nos piden:

- Para que x sea mayor que 20, y puesto que $x = 5 + 7k'$, basta elegir $k' \geq 3$. Tomando $k = 0$ y $k' = 3$ tenemos la solución $x = 26$, $y = -40$, $z = 3$.
- Para que z sea menor que -10, y puesto que $z = 3 + 4k$, necesitamos que $k \leq -4$. Elegimos $k = -4$, $k' = 0$ y tenemos la solución $x = 5$, $y = 23$, $z = -13$.
- Ahora hay que buscar una solución en la que tanto x como y sean mayores que 3. Para que x sea mayor que 3 basta con que $k' \geq 0$. Elegimos $k' = 0$, en cuyo caso $y = -13 - 9k$. Y para que sea mayor que 3 necesitamos $k \leq -2$. Entonces elegimos $k = -2$. Esto nos da la solución $x = 5$, $y = 5$, $z = -5$.
- Por último, puesto que $z = 3 + 4k$, no hay ningún valor de k para el que z sea múltiplo de 4. Por tanto, en este caso no hay solución.

2. Vamos a llamar x al número de paquetes que enviamos de `Tipo A`. En tal caso, el número de paquetes que enviamos de `Tipo B` es $17 - x$.

   Por otra parte, sea y el precio (en céntimos) de los paquetes `Tipo A`. Entonces, el precio de los paquetes `Tipo B` es $y + 35$.

   Ordenamos estos datos en el siguiente cuadro:

	`Tipo A`	`Tipo B`
Número de paquetes	x	$17 - x$
Precio paquete	y	$y + 35$
Dinero pagado	$x \cdot y$	$(17 - x) \cdot (y + 35)$

   El precio pagado en total es entonces $x \cdot y + (17 - x) \cdot (y + 35)$. Y esto último debe ser igual a 5450. Resolvemos entonces la ecuación $x \cdot y + (17 - x) \cdot (y + 35) = 5450$. Puesto que la cantidad de paquetes es un número entero, y la cantidad de céntimos también hemos de buscar soluciones enteras de esta ecuación.

   $x \cdot y + (17 - x) \cdot (y + 35) = 5450.$
   $x \cdot y + 17y + 17 \cdot 35 - x \cdot y - 35x = 5450.$
   $17y + 595 - 35x = 5450.$
   $17y - 35x = 4855.$
   $35x - 17y = -4855.$
   $35x \equiv -4855 \text{ mód } 17.$
   $x \equiv 7 \text{ mód } 17.$
   $x = 7 + 17k.$

   Pero como el número de paquetes `Tipo A` no puede ser mayor que 17 podemos asegurar que $x = 7$.

   Una vez calculado x, obtenemos y como

$$y = \frac{4855 + 35 \cdot 7}{17} = \frac{4855 + 245}{17} = \frac{5100}{17} = 300.$$

   En resumen:

   Tenemos 7 paquetes `Tipo A` y 10 paquetes `Tipo B`.

   Los paquetes `Tipo A` nos cuesta 3 euros enviarlos, y los paquetes `Tipo B` nos cuesta $3'35$ euros.

Ejercicio 3. *Sea* $m(x) = x^7+x^6+x^5+2x^4+x^3+2x^2+2x+1 \in \mathbb{Z}_3[x]$ *y* $q(x) = x^5+2x^4+2x^3+x+1 \in \mathbb{Z}_3[x]$.

1. *Calcula mcd*$(m(x), q(x))$.
2. *Factoriza* $m(x)$ *como producto de irreducibles.*
3. *En* $\mathbb{Z}_3[x]_{m(x)}$ *calcula, si es posible,* $(x^4+1)\cdot(2x^3+x^2+x+1)^{-1}$.

Solución:

1. Calculamos el máximo común divisor por medio del algoritmo de Euclides.

   - Dividimos $m(x)$ entre $q(x)$.

$$\begin{array}{c|cccccccc}
 & 1 & 1 & 1 & 2 & 1 & 2 & 2 & 1 \\
1 & & 1 & 1 & 0 & 2 & 2 & 1 & 2 \\
1 & & & 2 & 2 & 0 & 1 & 2 & \\
0 & & & & 1 & 1 & 0 & & \\
2 & & & & & & & & \\
2 & & & & & & & & \\
\hline
 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 0
\end{array}
\qquad
\begin{array}{l}
c(x) = x^2+2x+1 \\
r(x) = 2x^4+x^3+2x^2+2x
\end{array}$$

   - Dividimos $x^5+2x^4+2x^3+x+1$ entre $2x^4+x^3+2x^2+2x$.

$$\begin{array}{c|cccccc}
2 & 1 & 2 & 2 & 0 & 1 & 1 \\
\cline{1-1}
1 & & 1 & 2 & 2 & 0 & 0 \\
2 & & & 0 & 0 & 0 & \\
2 & & & & & & \\
0 & & & & & & \\
\hline
 & 1 & 0 & 1 & 2 & 1 & 1
\end{array}
\qquad
\begin{array}{l}
c(x) = 2x \\
r(x) = x^3+2x^2+x+1
\end{array}$$

   - Dividimos $2x^4+x^3+2x^2+2x$ entre x^3+2x^2+x+1.

$$\begin{array}{c|ccccc}
 & 2 & 1 & 2 & 2 & 0 \\
1 & & 2 & 1 & 1 & 0 \\
2 & & & 0 & 0 & \\
2 & & & & & \\
\hline
 & 2 & 0 & 0 & 0 & 0
\end{array}
\qquad
\begin{array}{l}
c(x) = 2x \\
r(x) = 0
\end{array}$$

   Y por tanto, $\text{mcd}(m(x), q(x)) = x^3+2x^2+x+1$.

2. Puesto que x^3+2x^2+x+1 es un divisor de $m(x)$, dividimos $m(x)$ entre este polinomio:

$$\begin{array}{c|cccccccc}
 & 1 & 1 & 1 & 2 & 1 & 2 & 2 & 1 \\
1 & & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\
2 & & & 2 & 1 & 1 & 2 & 2 & \\
2 & & & & 2 & 1 & 1 & & \\
\hline
 & 1 & 2 & 2 & 1 & 1 & 0 & 0 & 0
\end{array}$$

   Luego $m(x) = (x^4+2x^3+2x^2+x+1)\cdot(x^3+3x^2+x+1)$.

   Ahora factorizamos cada uno de estos dos polinomios.

   - Factorizamos $q_1(x) = x^4+2x^3+2x^2+x+1$.
     Tenemos que $q_1(0) = 1$, $q_1(1) = 1+2+2+1+1 = 1$, $q_1(2) = 2^4+2\cdot 2^3+2\cdot 2^2+2+1 = 16+16+8+2+1 = 43 = 1$, luego $q_1(x)$ no tiene raíces.
     Probamos a dividir por los irreducibles de grado 2, que son x^2+1, x^2+x+2, x^2+2x+2.

$$\begin{array}{c|ccccc}
 & 1 & 2 & 2 & 1 & 1 \\
0 & & 0 & 2 & 1 & 2 \\
2 & & & 0 & 0 & \\
\hline
 & 1 & 2 & 1 & 2 & 0
\end{array}
\qquad\qquad
\begin{array}{c|ccccc}
 & 1 & 2 & 2 & 1 & 1 \\
2 & & 2 & 1 & 1 & 2 \\
1 & & & 2 & 1 & \\
\hline
 & 1 & 1 & 2 & 0 & 0
\end{array}$$

$$\begin{array}{c}
c(x) = x^2+2x+1 \\
r(x) = 2x
\end{array}
\qquad\qquad
\begin{array}{c}
c(x) = x^2+x+2 \\
r(x) = 0
\end{array}$$

     Y vemos que $x^4+2x^3+2x^2+x+1 = (x^2+x+2)^2$.

- Factorizamos $q_2(x) = x^3 + 2x^2 + x + 1$.
  $q_2(0) = 1$, $q_2(1) = 1 + 2 + 1 + 1 = 2$, $q_2(2) = 2^3 + 2 \cdot 2^2 + 2 + 1 = 8 + 8 + 2 + 1 = 19 = 1$. Por tanto, $q_2(x)$ no tiene raíces, y al ser de grado 3 podemos concluir que es irreducible.

La factorización de $m(x)$ nos queda entonces $m(x) = (x^2 + x + 2)^2 \cdot (x^3 + 2x^2 + x + 1)$.

3. En primer lugar comprobamos si existe $(2x^3 + x^2 + x + 1)^{-1}$. Para esto, calculamos $\mathrm{mcd}(m(x), 2x^3 + x^2 + x + 1)$.

$$\begin{array}{r|cccccccc}
2^{-1} = 2 & 1 & 1 & 1 & 2 & 1 & 2 & 2 & 1 \\
\hline
-1 \cdot 2 = 1 & & 1 & 1 & 1 & 2 & 1 & 0 & 1 \\
-1 \cdot 2 = 1 & & & 2 & 2 & 1 & 0 & 1 & \\
-1 \cdot 2 = 1 & & & & 1 & 0 & 1 & & \\
\hline
 & 1 & 2 & 1 & 0 & 1 & 1 & 0 & 2
\end{array}$$

$c_1(x) = 2 \cdot (x^4 + 2x^3 + x^2 + 1) = 2x^4 + x^3 + 2x^2 + 2$

$r(x) = x^2 + 2$

$$\begin{array}{r|cccc}
 & 2 & 1 & 1 & 1 \\
0 & & 0 & 2 & 1 \\
1 & & & 0 & \\
\hline
 & 2 & 1 & 0 & 2
\end{array}$$

$c_2(x) = 2x + 1$

$r_2(x) = 2$

Puesto que el último resto (que es 2) no es un polinomio mónico, lo multiplicamos por $2^{-1} = 2$ y concluimos que $\mathrm{mcd}(x^7 + x^6 + x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1, 2x^3 + x^2 + x + 1) = 1$. Por tanto, existe el inverso que buscamos.

A partir de las divisiones efectuadas tenemos la siguiente tabla:

$x^7 + x^6 + x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1$		0
$2x^3 + x^2 + x + 1$		1
$x^2 + 2$	$2x^4 + x^3 + 2x^2 + 2$	$v_1(x)$
2	$2x + 1$	$v_2(x)$
1		$2 \cdot v_2(x)$

Calculamos $v_1(x)$, $v_2(x)$ y $2 \cdot v_2(x)$.

$v_1(x) = 0 - 1 \cdot (2x^4 + x^3 + 2x^2 + 2) = x^4 + 2x^3 + x^2 + 1$.
$v_2(x) = 1 - v_1(x) \cdot (2x + 1) = 1 + (x + 2) \cdot (x^4 + 2x^3 + x^2 + 1) = x^5 + x^4 + 2x^3 + 2x^2 + x$.
$(2x^3 + x^2 + x + 1)^{-1} = 2 \cdot v_2(x) = 2x^5 + 2x^4 + x^3 + x^2 + 2x$.

Una vez calculado el inverso, lo multiplicamos por $x^4 + 1$.

$$\begin{array}{cccccccccc}
 & & & & 2 & 2 & 1 & 1 & 2 & 0 \\
 & & & & & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & & 2 & 2 & 1 & 1 & 2 & 0 \\
2 & 2 & 1 & 1 & 2 & 0 & & & & \\
\hline
2 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 0
\end{array}$$

Y ahora dividimos el resultado por $x^7 + x^6 + x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1$.

$$\begin{array}{r|cccccccccc}
 & 2 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 0 \\
2 & & 1 & 1 & 2 & 1 & 2 & 2 & 1 & 0 & 1 \\
2 & & & 0 & 0 & 0 & 0 & 0 & 0 & 2 & \\
1 & & & & 1 & 1 & 2 & 1 & 2 & & \\
2 & & & & & & & & & & \\
1 & & & & & & & & & & \\
1 & & & & & & & & & & \\
2 & & & & & & & & & & \\
\hline
 & 2 & 0 & 2 & 1 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}$$

Luego $(x^4 + 1) \cdot (2x^3 + x^2 + x + 1)^{-1} = x^6 + x^3 + x^2 + x + 1$.